15 Internet in Automation and Process Control Systems

BABU JOSEPH AND DEEPAK SRINIVASAGUPTA

INTRODUCTION

The Internet is a loose collection of networked computers and smaller devices (e.g., personal digital assistant) distributed globally but linked together through a set of communication channels including fiber-optic cables, satellite communication systems, coaxial cables, wireless connections, and telephone wires. These computers and devices communicate with each other through a set of well-defined protocols generally referred to as transmission control protocol (TCP)/Internet protocol (IP). Each of these individual computers or devices can be termed as network hosts or nodes.

A layperson's way of understanding the Internet would be to view it similar to a postal service. The Internet accepts messages (i.e., digital data containing text, images, files, etc.) with a delivery address associated with the message. The TCP/IP protocol takes care of finding various paths to the delivery address and delivering the message to the intended recipient. One major difference between the postal service and Internet analogy is that the Internet does not keep the message intact. Rather, it is broken up in to small manageable pieces called frames. Each of them is routed to the recipient. At the destination, the frames are reassembled in the proper order before the message is delivered.

The Internet has evolved over the years, starting as a small research project initiated by the U.S. Advanced Research Projects Agency (ARPA) in the 1960s. Eventually the government got out of the business of running this network (originally called the ARPANET) and allowed it to be commercialized, starting in the 1980s. Currently there are millions of computers and smaller devices connected to the Internet directly or indirectly through cable, telephone wires, wireless networks, or satellite systems allowing people and machines to communicate with each other.

The Internet is similar to the open system interconnection (OSI) network model. The OSI model is a standardized conceptual framework consisting of seven layers (Figure 15.1). Each layer provides a characteristic set of functions, and provides service to the layer directly above it. Protocols constitute the "language" that enables entities (at the same layer) in network hosts to interact with each other. All of these seven layers may be found in a host connected to the network, such as a computer connected to the Internet. The figure identifies all seven layers, as well as examples of these layers in the Internet.

For instance, IP is a common network protocol that has been used for packet routing over a packet-switched network such as the Internet. Packet-switched networks do not maintain a persistent connection between the two end systems, as opposed to circuit switched networks (e.g., traditional wired telephones). Instead, data are encapsulated in packets, addressed, and sent out to the receiver. Of the two most popular transport protocols over IP networks, TCP is a connection-oriented protocol whereas universal datagram protocol (UDP) is a faster connectionless protocol [1]. TCP guarantees reliable two-way communication with error-free delivery using retransmissions and acknowledgements. UDP is more suitable for loss-tolerant real-time multi-media applications.

Most of the communication on the Internet is based on a client–server paradigm, where one network host acts as a service provider (server) to another host that requests that service (client). The server is always on and connected to the network. It awaits incoming requests. The client initiates the contact with the server. An example of this is a person visiting a web portal using a desktop computer. In this case, the desktop acts as the client, initiating a request to a remote server to transmit a certain web page.

Although there is large flexibility built into the connection paths between any two points on the Internet (there are millions of possible pathways), there is no guarantee of service on Internet. Messages are not guaranteed to arrive with certainty of time. Network traffic is unpredictable and therefore delivery times are random. Herein lies the crucial issue when we think of using the Internet in process control and automation. Secondly, there is also security risk involved in the handling of the message. Although the protocols have evolved over the years to allow increased security of the messages transmitted through Internet, the open nature of the network connection implies that hackers can and will try to break in and gain unauthorized access.

These two critical concerns, that of security and guaranteed delivery, have prevented companies from migrating completely to the Internet for process control applications. However, the ubiquity of the Internet, its ease of access and use, and the globalization of manufacturing and business enterprises have led to increased use of Internet for integrating plant level communication networks with business

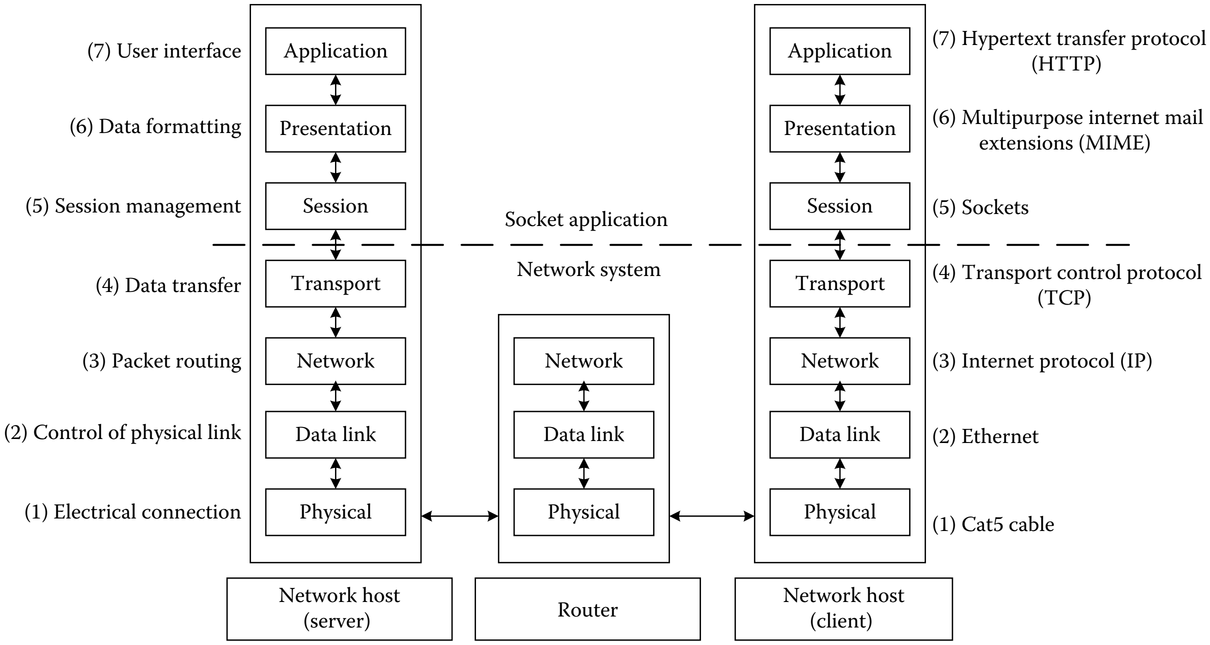

FIG. 15.1
The OSI network model.

enterprise–related functions. In this article, we shall examine the evolution of the use of Internet for process control, how it is used today, and some future trends.

The article consists of the following sections: the section "Evolution of Digital Process Control and Automation Systems" examines the evolution of process control systems briefly from stand-alone controllers to the modern-day distributed control systems and programmable logic controllers control systems, with particular emphasis on the networking functionalities. This section also examines the evolution of the business enterprise and how the data and communication networks of business enterprise systems are integrated. The section "Convergence of Internet and Process Automation Systems" focuses on the convergence of the two networked technologies as companies try to take advantage of the globalization of business and manufacturing enterprise systems. The section "Future" looks at future trends in the evolution of control and communication systems as they try to merge with the Internet.

EVOLUTION OF DIGITAL PROCESS CONTROL AND AUTOMATION

Digital computers began to be used in process control applications starting in the 1960s. The early use of computers was primarily in the supervisory mode, as a device to capture, store, and display data originating from the analog process sensors and controllers. With the arrival of the microprocessor, distributed computer control became feasible. The 1970s saw the development and deployment of microprocessor-based DCS such as Honeywell TDC2000 series in the continuous process industry and PLCs in batch and discrete manufacturing industry. DCS refers to a plant control architecture where the control elements are distributed throughout the process/system, and are networked to a central supervisory controller for communications and monitoring. PLCs are specialized industrial computers mainly used for control of discrete manufacturing systems with multiple inputs and outputs. These systems featured proprietary process control networking systems to link together the various microprocessor-based devices including local control units, operator stations, and engineering work stations. Communications were handled through data highway cables using protocols that were developed by the system manufacturer. These data highways eventually evolved into local area networks (LAN) that also were proprietary. These control-oriented LANs were designed specifically to handle the real-time nature of the system and paid considerable attention to redundancy and reliability while ensuring timely delivery of messages among the devices attached to the network. These devices were isolated from the business networks and hence provided inherent security from unauthorized users. Figure 15.2 shows the architecture of a typical plant control network system used in DCS.

Meanwhile, the networking of business enterprise systems also evolved from centralized business computing to distributed client–server architecture. While a number of proprietary networking systems existed at first, the Ethernet networking became the de facto standard and eventually most office systems adopted this Ethernet LAN strategy. During the 1990s, the need to integrate manufacturing with business was recognized as a critical need and therefore the push began toward integrating the computer networks used

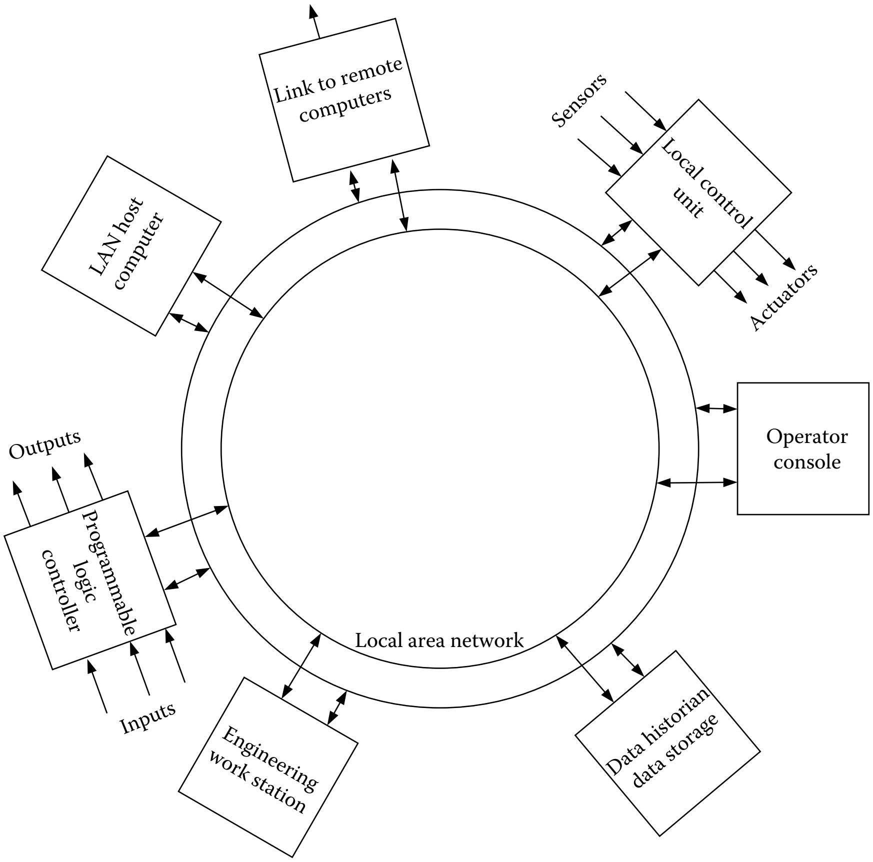

FIG. 15.2
LAN system architecture for DCS systems.

for process control and manufacturing automation with the wide area networks (WAN) used for linking the various components of the business enterprise. The globalization of manufacturing and business also provided the necessary impetus to develop integration of the distributed manufacturing operations with business operations. Initially large companies set up computer networks that were insulated from the outside world. The rapid evolution of the Internet and the ease of communication using off-the shelf computers with the Internet led to the adoption of the Internet itself as the WAN used by many companies to link worldwide operations. So the demand to share process data and information instantaneously with business managers and customers led to the need to develop communication channels between the proprietary LANs used by DCS/PLC systems and the Internet.

At the same time, we saw a huge investment by companies in company-wide data and information handling software systems that promised to make all data available to all users as soon as possible. Such enterprise resource planning (ERP) systems such as PeopleSoft, Axapta (now Microsoft Dynamics AX), SAP, Great Plains (now Microsoft Dynamics GP), and Oracle Applications were built around large data base management systems to facilitate easy assimilation, organization, and distribution of data and information starting at the plant level, through the business operations to the customer. ERP systems are considered as "back-office" systems (in contrast to "front-office" systems such as customer relationship management systems (CRM) that cover more than one core function of an enterprise. ERP systems are usually modular, with separate modules for functions such as human resources, payroll, accounting, asset management, and inventory management. ERP systems started communicating with other systems such as CRM or supply chain management, in some cases, even taking over their functions. Computer-integrated manufacturing was becoming a reality.

Meanwhile another evolution was taking place at the process control level. The ever decreasing cost of computing and the increased demand for improved data collection devices led to the development of intelligent sensors and actuators with built-in capability for data validation and self calibration and information processing. This meant that these devices also had to be networked. After some initial proprietary networking development, manufacturers began to adopt *sensor networking standards*. A few standards such as MODBUS and PROFIBUS evolved and were adopted by a large number of control system vendors and manufacturers. The biggest gain was in the reduction of wiring that had to be done to hook up these sensors and actuators to the local control units. Figure 15.3 shows the structure of a typical device-level network.

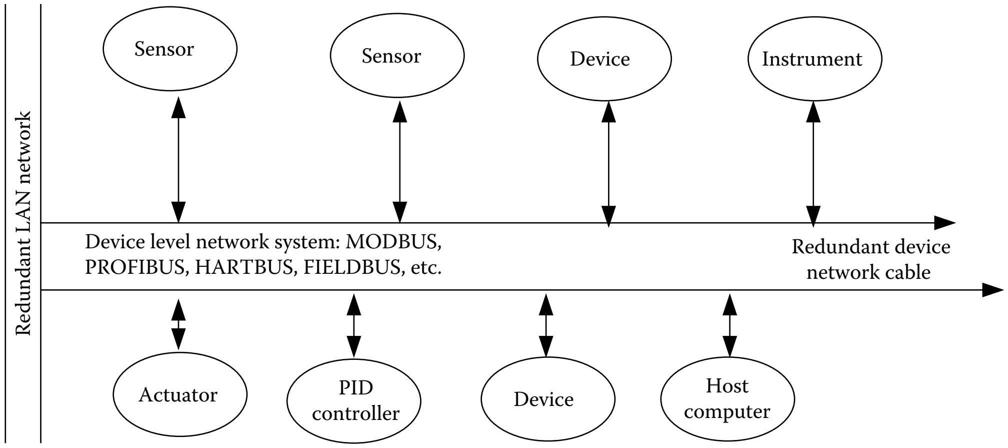
Redundant LAN network
Sensor
Sensor
Device
Instrument
Device level network system: MODBUS, PROFIBUS, HARTBUS, FIELDBUS, etc.
Redundant device network cable
Actuator
PID controller
Device
Host computer

FIG. 15.3
Device-level networking for sensors, actuators, instruments, and other devices.

CONVERGENCE OF INTERNET WITH PROCESS AND AUTOMATION

The widespread acceptance of the Internet as a medium of communication and the explosive growth of hardware and software that support it made it inevitable that process control network (PCN) systems began to adapt to its usage.

Security Issues

The concerns rose above regarding guaranteed delivery time and security still prevents the Internet from replacing the PCN as the communication medium. Rather, the adoption has progressed slowly and with deliberate caution. Use of IP-based protocols does bring its own issues, related to robustness and quality of service. This has triggered a need for research in fault detection and identification [2] and security [3]. Tinham [4] reports that security experts at the British Columbia Institute of Technology (BCIT) and their collaborators report a tenfold increase in successful attacks on process control and supervisory control and data acquisition systems since 2001. Byres [5] notes that industrial controls has borrowed substantially from the world of information systems over the last few years; while technologies such as Ethernet and TCP/IP have made the interfacing of industrial equipment much easier, there is now significantly less isolation from the outside world, with the result that network security problems from the business network can be passed on to the process network, putting industrial production and human safety at risk.

Figure 15.4 shows the current state of the art. The Internet is used as a medium for communicating data and information when delivery time is not critical. At best, Internet has been most effective for process monitoring and supervisory control as opposed to the lowest form of control proportional-integral-derivative (PID) control. Secure gateways and encrypting techniques are used to protect the data and information during its transmission through the Internet.

The client–server architecture is used invoking ERP type software to provide data and information while functionalities related to regulation and real-time control are retained within the PCN. Rather the PCNs become clients to ERP software to generate near real-time data and reports that are then made available to all properly authenticated clients globally distributed on the Internet. The data and information could be provided through web pages and/or report on demand. Such data and information are then available to customers, sales teams, managers, and business planning teams. Engineers can also access data for monitoring but with additional privilege to change or update software and algorithms residing on the PCN. In some instances permission may also be granted to authenticated personnel to run higher level control functions such as optimization of plant settings with the approval of plant personnel.

Secure gateways and data encryption procedures are essential to provide security against unauthorized and illegal break-ins. The virtual private network (VPN) is one of the schemes currently used to create secure gateways for linking proprietary networks through the Internet. Readers can refer to Chapter 32 for more information on the VPN.

In addition to this, less secure networking has been proposed by completing bypassing the PCN and providing devices with IP addresses and then using the Internet for communication with the device. An example of that is a standalone PID controller with an IP address and Ethernet communication built-in, which can be connected to the Internet directly. Clients can then interrogate the controller regarding current data and status and make modifications to the set points, change tuning parameters, and even take manual control remotely if needed. Needless to say, such a system is risky for most applications where security and safety concerns override the convenience of remote access and manipulation.

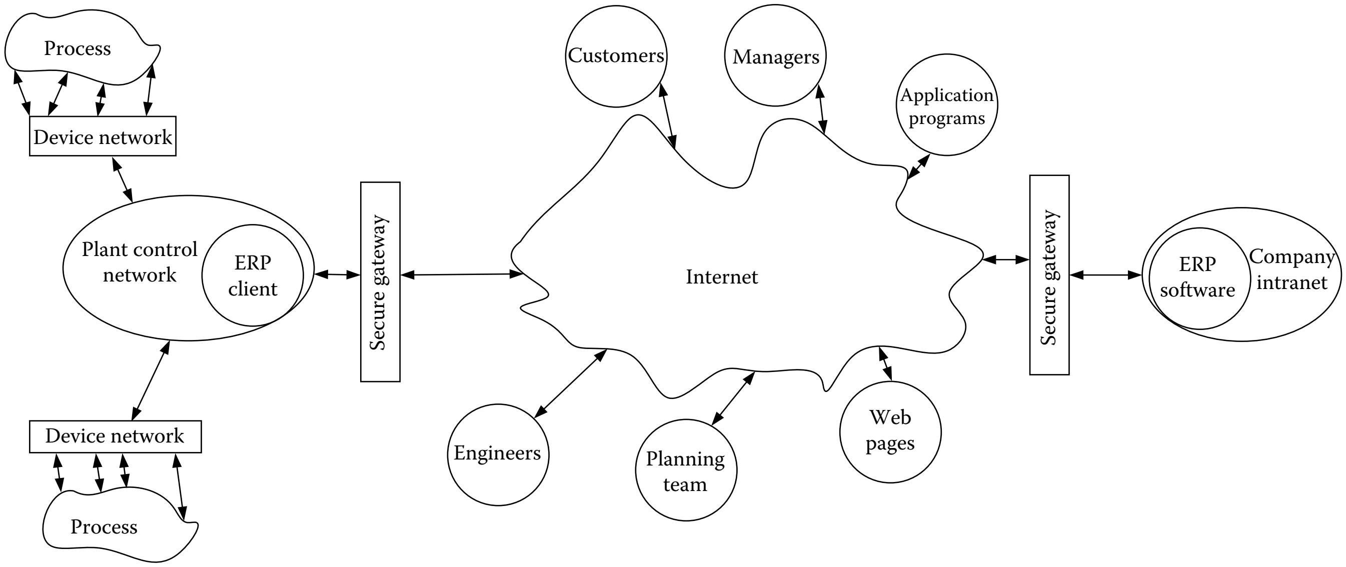

FIG. 15.4
State of the art in convergence of Internet and process automation systems.

Advent of IPv6 and IPSec

As mentioned earlier, the Internet uses a protocol known as IP to move data between nodes. Over the years, this protocol has evolved. Currently most systems are running version 4 of the protocol known as IPv4. Two new releases of the protocol, IPv6 and IPsec address some of the concerns expressed above. The Internet Protocol Security (IPsec) is a framework of open standards developed by the by the Internet Engineering Task Force for protecting communications over IP networks. IPsec was developed alongside IPv6 and is required in all standards-compliant implementations of IPv6. IPsec is also available as an optional add-on to IPv4, and accounts for most of its use today. Because IPsec operates at the lower, IP level, it provides a secure foundation that higher-layer protocols in the OSI network model to benefit from it. For additional knowledge, IPv5 has never been released and implemented.

The evolution of IPv6 has been recognized for its intent to address the anticipated exhaustion of the IP address space with IPv4. Unlike the 32-bit addressing scheme of IPv4, IPv6 uses 128 bits, resulting in 2^{128} or 3.4×10^{38} unique addresses. This also means that any individual device can have its own unique IPv6 address, and reduce reliance on workarounds such as network address translation (NAT) to alleviate IPv4 depletion.

Feedback Control over the Internet

Real-time feedback control over the Internet will be restricted to niche applications. For the most part, remote processes will likely have some autonomous control built-in. Such an approach will improve control performance and process stability, especially for fast acting processes (Figure 15.5). Use of the Internet for distance learning around automation and control has been illustrated in a number of academic studies by Srinivasagupta and Joseph [6], Kennepohl et al. [7], and Baran et al. [8].

Since the Internet is a packet switched network, the time delay at each node on the network has been modeled [1] as

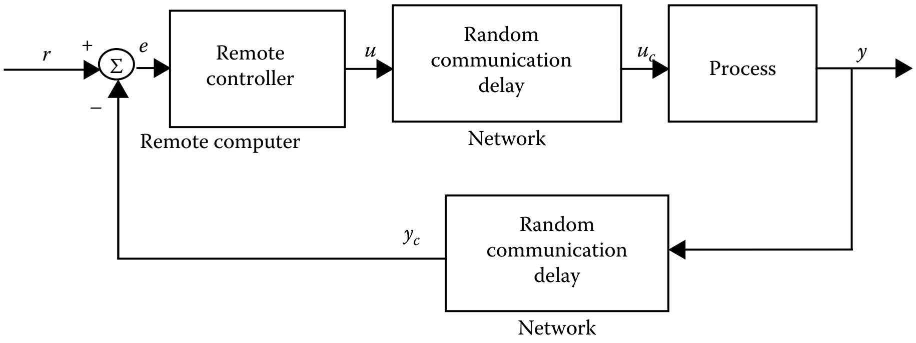

FIG. 15.5
Feedback structure with communication delays

arising from four components: the processing delay, the queuing delay, the transmission delay, and the propagation delay. The round-trip time (time taken for a data packet to travel from the controller to the process and back) is variable on the Internet and is of the order of milliseconds. In principle, communication delays have been widely known to degrade performance of control systems. In general, this is not an issue for the majority of processes where the process time constants (minutes, hours, and days) are larger than the communication delays (milliseconds). In cases where this can be a concern (e.g., fast acting electrical systems), the preferred approach is to incorporate local feedback control so as to take the delays and their variability out of the control equation. As noted by a number of sources (e.g., [9]), most control operations in industrial applications can tolerate latencies or delays of 10–50 ms.

There has also been research into control algorithms that address the latency and reliability issues in networked control systems (e.g., [10]) where the feedback controller is remotely located from the process. In these examples, the process and the feedback controller use the Internet as a communication medium. Time-stamping of data packets has been shown to be an important factor in the development of such control algorithms, and has even been provisioned in newer network architectures such as WirelessHART.

Monitoring and Supervisory Control over the Internet

Many industrial control systems have features for access over the Internet. As opposed to real-time feedback control, these features are intended for enterprise-wide visibility and monitoring purposes. Supervisory control and monitoring over the Internet is often used rather than real-time feedback control.

It is now possible to access process setups and instruments remotely and gain access to real-time data anytime anywhere. Laboratory instrumentation software such as Labview provides Internet-mediation capabilities. A Labview virtual instrument can be easily set up for access over the Internet. Access to analytical instruments is thus now possible using an ordinary web browser. Internet-mediation features are also being incorporated into various engineering and manufacturing software for various purposes.

Interconnection of Business and Manufacturing Systems

Integration of business and manufacturing operation may be regarded as a “holy grail.” While business systems consist of basic accounting systems, and perhaps more sophisticated ERP software, manufacturing systems consist of lower level measurement and control networks. A manufacturing company with multiple production locations usually has one or few business systems such as CRM or ERP software but multiple manufacturing systems (one at each location). In other words, the manufacturing systems are generally spatially contained to a certain plant, whereas one ERP system exists for the entire geographically distributed enterprise. The management of the ERP system is usually done by the corporate information technology (IT) personnel, whereas the manufacturing control system is maintained by a combination of plant-level IT and instrumentation personnel.

Integration of ERP systems with plant control networks will provide instantaneous access to data to engineering and business functions in the company. For instance, corporate managers can immediately be notified of significant downtime or abnormal events at a manufacturing operation that can significantly affect the bottom line. Forecasting modules in ERP software can analyze different scenarios arising from plant operations. At the same time, corporate engineering personnel can use sophisticated software for loop monitoring, performance monitoring, sensor integrity, control system performance monitoring, and process optimization residing on remote distributed computers communicating via the Internet. Middleware such as Microsoft BizTalk server make integration of disparate systems possible through “adapters” or “drivers” that connect with different software.

RFID Technology

The areas of business-to-business (B2B) e-commerce and supply chain visibility have significantly benefited from the widespread penetration of the Internet. Occurring at the enter-company level, for instance, these technologies allow a supplier to monitory raw material inventory levels at one of its corporate customers securely over the Internet, automatically dispatching replenishments in accordance with a long-term supply contract. Several technologies have made this possible. The radio frequency identification (RFID) technology has one emerged network-based technology impacting factory automation and supply chain. RFID technology is in essence a system to improve visibility in the supply chain. RFID tags are seen as a replacement to the prevailing barcode technology. Unlike the older bar codes that store limited, one-time information, RFID tags consist of a microchip and a radio antenna. Hence, RFID tags can store much more information, such as country of origin, date of manufacture, batch/lot information, expiration dates, or ingredient information. This technology also overcomes other difficulties with bar codes such as line of sight issues, range, and the ability to rewrite information.

In 2003, Wal-Mart directed its top 100 suppliers to start putting RFID tags on in-bound shipments. Likewise, organizations such as the U.S. Department of Defense, Hewlett Packard, Airbus Industries, and Boeing Corporation are engaged in RFID implementations in their operations.

RFID technology comes in two main flavors: active and passive. Active RFID tags (costing tens of U.S. dollars) contain a small battery, and can act as small radio beacon. This makes them useful for applications such as asset tracking. Implementations of active RFID tags include hospital settings when they are used to track expensive life-saving equipment throughout a building. Priced in several cents based on volume, passive RFID tags are much cheaper (though currently more expensive than bar code technology), and can be interrogated only by readers. Some RFID tags can even incorporate sensor such as for tracking temperature, which this makes them very useful for applications such as tracking refrigerated products. Limitations of RFIDs include difficulties around metals and water, something that is the subject of research today. RFID and Internet are used in many other applications such as asset tracking, ecosystems, and wireless embedded internet devices, and control systems.

FUTURE

Security and Performance

Security and performance issues will continue to be important issues into the future. This is particularly important as the cyberspace is regarded as the new frontier of warfare in the twenty-first century. Instances of denial of service attacks in the past decade have only reinforced vulnerabilities of today's cyber infrastructure, and the potential havoc those attacks can have on systems, especially with greater integration into the future. The expansion of the consumer Internet into newer geographical and political jurisdictions, and increase in broadband access only mean that an increasing number of hosts are connected to the Internet on a near-permanent basis. Individual devices are being directly addressable, and many come with embedded web servers. This extends to the availability of networked PID controllers operating on the Internet.

In previous years, plant-level automation and security infrastructure enjoyed security by virtue of isolation, anonymity, and their proprietary nature. As those barriers come down, security has been recognized as a greater concern and has been the subject of much research interest. Today, security is multilayered, with firewalls between the plant network, and the company's IT infrastructure. Another layer of security is also required between the company and the outside.

Security will continue to remain a prime concern into the future. Both academia and the industry have recognized security to be a priority. In September 2009, the U.S. Department of Homeland Security released the "Roadmap to Secure Control Systems in the Chemical Sector" prepared by the Chemical Sector Roadmap Working Group. The development of this roadmap for the chemical sector is part of a broader effort to guide the efforts of individual sectors in securing their industrial control systems. Alongside security, privacy is also regarded as an emerging concern with legislation in several jurisdictions impacts this subject. This will impact emerging technologies such as RFIDs and mobile devices that will need to balance the often competing interests between security and privacy.

Wireless Networks

An area of interest is the wireless networks as they are of used in conjunction with the internet. Wireless devices and networks have been particularly attractive for retrofits to existing plants. It has been reported [10] that wiring costs exceed the cost of the control components being installed. Typical wireless devices in a plant use openly available the industrial, scientific, and medical (ISM) radio frequency bands.

However, wireless infrastructure does not come without challenges. The growth in wireless infrastructure only adds another dimension of difficulty as far as security is concerned. Radio waves cannot be contained unlike hard-wired electrical signals. Manufacturing plants contain significant amounts of metal in process equipment, piping, and industrial machinery. The metal causes significant reflections, degrading communications quality. As more and more devices get on the limited bandwidths made available by the spectrum regulators, the wireless nodes face increasing interference, and the quality of service can only deteriorate. Security of wireless networks is another issue, as the electromagnetic waves used can be picked up by any receiver. Generally, protection is provided through data encryption.

Industry standards have started to emerge in the wireless domain and have started to address security and performance issues. For instance, in 2007, the HART Communications Foundation (http://www.hartcomm.org) released the Highway Addressable Remote Transducer (HART) Protocol version 7.0 with support for WirelessHART. As claimed by the HART Communication Foundation, the WirelessHART standard is the first open wireless communication standard for measurement and control in the process industries. It uses wireless mesh networking between field devices (i.e., every WirelessHART device is a router, operating off the power from a power line or battery), with built-in 128 bit Advanced Encryption Standard security over the 2.4 GHz license-free ISM radio band. WirelessHART hops between the channels on the 2.4 GHz band to avoid interference from other sources using channels on the same band. Likewise, from the International Society of Automation (ISA), the ISA100 standards committee has been developing a comprehensive standard for industrial wireless communications. The first release from this organization is ISA100.11a, intended for process data acquisition and limited control needs in the process industries [11].

Another important development is the creation of the ZigBee specification by the ZigBee Alliance—an open global wireless standard for low-cost, low-power, wireless measurement and control networks. It is based on the IEEE 802.15.4 packet-based radio specification and uses unlicensed bands in different countries.

An increasing number of manufacturing plants (e.g., cryogenic air separation units) are now being operated unattended and remotely. The network becomes a means for instance, for control engineers employed in corporate headquarters to do optimization and supervisory control over the Internet. Likewise, field and sales personnel can access the plant with cellular phones and other mobile devices to interrogate inventory and product quality. Increasing levels of feedback control (including model predictive control) are being embedded into local control devices.

Smart Sensor Standards

Smart sensors is the term used to describe transducers (or even actuators) that not only provide a basic function such as measurement, but can also provide additional functions such as indicative health information. During this last decade, the IEEE 1451 Smart Sensor family of standards has been developed, with the purpose of making it easier for sensor and transducer manufacturers in developing intelligent devices, to interface those devices to networks, systems, and instruments. At the heart of the IEEE 1451 standard family is the transducer electronic data sheets, an electronic datasheet attached to the transducer, storing identification, calibration, correction data, measurement range, and manufacturer-related information. It may be anticipated that an increasing number of new devices and sensors will enter the marketplace compliant with these standards.

Adaptation of Internet Technology

IP is rapidly being introduced into control system networks. This enables standardization easily and readily. Consumer and business Internet represents much larger market space than specialty process control and automation markets. The former provides a certain economy of scale that has lowered the cost of technology to levels affordable by the lay person. Such economies of scale only make it natural for consumer Internet technologies to be adapted to the plant floor. Adapting TCP/IP/Ethernet technologies from the larger consumer/business IT sector into the plant floor is not straightforward.

Manufacturing environments are often noisy, dirty, have extremes of temperatures, vibration, and prone to severe interferences (electrical, auditory, etc.). Traditional technology will need to be adapted by incorporating considerations such as robustness. Applicable standards such as those set by the International Electrotechnical Commission (IEC) and/or National Electrical Manufacturers Association need to be complied with. For example, IEC 60529 provides for the IP Code (or International Protection Rating) that addresses varying levels of protection provided by enclosures.

The development of industrial Ethernet is an example of such adaptation. Ethernet as a link-layer protocol has been adapted for plant-level communications, by incorporating increased robustness. High-speed Ethernet, though fast-acting switches that can prioritize network traffic (and thereby offer or quality of service), has made some of this attractive. Industrial Ethernet differs from traditional Ethernet in that the hardware used is designed for harsh environments. A recent ARC Advisory Group study found that Industrial Ethernet devices grew at more than a 50% annual rate from 2001 to 2003 [9]. Many application-level industrial control protocols (e.g., Modbus) have started to become accessible over the IP suite (TCP/IP riding on top of industrial Ethernet).

Interoperability and Harmonization

With increased globalization in this century, we may expect a greater harmonization across technologies as they relate to automation and control. The previous century saw competing proprietary technologies and "bus wars" (e.g., Foundation Fieldbus popular in Europe, HART popular in North America). As noted in InTech [12], most companies are global and would rather have one standard on a particular topic, rather than one for North America, one for Europe, and one for Asia. The article also notes that manufacturing and engineering work forces are now global, so the practices employed in design and implementation must also translate to a broad and diverse audience.

This emerging reality has not been lost upon the various organizations in the automation and process control world. For instance, in recent years, the Fieldbus Foundation (http://www.fieldbus.org), HART Communication Foundation, and PROFIBUS Nutzerorganisation e.V. (with the subsequent addition of the OPC Foundation in 2005) have created a joint working group to expand capabilities of the electronic device description (EDD) technology. Similarly, the three-part IEC 62443 working group on control system security TC65 WG 10 have unanimously voted to take their work to ISA-SP99 WG4 for further development. The joint effort on control system security would produce an ISA standard and an IEC technical specification, as reported by Policastro [13]. Another important series of standards for interoperability is OPC. Formerly, abbreviated for object linking and embedding (OLE) for process control, OPC today enables open connectivity via a series of open standards. OPC standards enable communication of real-time data between control products from different companies, and uses Microsoft's OLE technology.

Interoperability and harmonization for automation and process control hardware and software will be important in this century. Globalization and the need for increased economies of scale will be key drivers toward this trend.

References

1. Kurose, J.F. and Ross, K.W., *Computer Networking: A Top-Down Approach Featuring the Internet*, Addison Wesley Publishing Company, Reading, MA, 2000.
2. Park, B., Won, Y.J., Yu, H., Hong, J.W.-K., Noh, H.-S., and Lee, J.J., Fault detection in IP-based process control networks using data mining, *IFIP/IEEE International Symposium on Integrated Network Management*, June 1–5, 2009, Long Island, NY, pp. 211–217, 2009.
3. Ryu, D.H., Kim, H.J., and Um, K., Reducing security vulnerabilities for critical infrastructure, *Journal of Loss Prevention in the Process Industries*, 22, 6, 1020–1024, November 2009.
4. Tinham, B., Your manufacturing plant is not immune to attack, *Manufacturing Computer Solutions*, 11, 5, 32–34, 2005.

5. Byres, E., Carter, J., Elramly, A., and Hoffman, D., Worlds in collision—Ethernet and the factory floor, ISA 2002 Emerging Technologies Conference, *Instrumentation, Systems and Automation Society*, Chicago, October 2002.
6. Srinivasagupta, D. and Joseph, B., An internet-mediated process control laboratory, *IEEE Control Systems Magazine*, 23, 1, 11–18, 2003.
7. Kennepohl, D., Baran, J., Connors, M., Quigley, K., and Currie R., Remote access to instrumental analysis for distance education in science, *International Review of Research in Open and Distance Learning*, 6, 3, 2005, ISSN: 1492-3831, http://www.irrodl.org/index.php/irrodl/article/view/260/404.
8. Baran, J., Currie, R., and Kennepohl, D., Remote instrumentation for the teaching laboratory, *Journal of Chemical Education*, 81, 12, 1814–1816, 2004.
9. *Industrial Ethernet: A Control Engineer's Guide*, A White Paper by Cisco Systems, Inc., San Jose, CA, August 2003 (published by Instrument Society of America, Research Triangle Park, Raleigh, NC).
10. Srinivasagupta, D., Joseph, B., Schättler, H., Time-stamped model predictive control: An algorithm for control of processes with random delays, *Computers and Chemical Engineering*, 28, 8, 1337–1346, 2004.
11. Caro, D., Wireless networking in plant, *InTech*, May 2009.
12. Policastro, E.F., Multiple regional vs. one global standard, *InTech*, May 1, 2007.
13. Policastro, E.F., Security standard hopes to go global, *InTech*, April 1, 2007.